CLAIMS

What is claimed is:

1. An apparatus comprising:

an embedded firmware agent having instructions that cause the embedded firmware agent to selectively operate in a management mode during which a host operating system relinquishes control of a host system in which the embedded firmware agent resides;

an embedded controller agent that operates independently of the host operating system and selectively invokes the management mode, the embedded controller agent having a network interface to allow the embedded controller agent to communicate over a network independently of the host operating system; and

a bi-directional agent bus coupled between the embedded firmware agent and the embedded controller agent to transmit messages between the embedded firmware agent and the embedded controller agent.

2. The apparatus of claim 1 further comprising a trusted module coupled with the embedded firmware agent and the embedded controller agent, the trusted module to perform cryptographic operations to support operations by the embedded controller agent.

3. The apparatus of claim 1 wherein the embedded controller agent asserts a management interrupt signal to invoke the management mode.

4. The apparatus of claim 1 wherein the embedded controller agent and the embedded firmware agent interact to provide manageability features to the host system.

5. The apparatus of claim 4 wherein the manageability features are provided prior to the host operating system being loaded.

6. The apparatus of claim 4 wherein the manageability features are provided after the host operating system has been loaded.

7. The apparatus of claim 4 wherein the manageability features are provided concurrently with loading of the host operating system.

8. The apparatus of claim 4 wherein the manageability features comprise host operating system independent update of a flash memory device via the embedded controller agent.

9. The apparatus of claim 4 wherein the manageability features comprise monitoring of host functionality and reporting to a remote device via the embedded controller agent.

10. The apparatus of claim 4 wherein the manageability features comprise providing boot services to the host system via the embedded controller agent.

11. The apparatus of claim 4 wherein the manageability features comprise providing emergency runtime services via the embedded controller agent.

12. The apparatus of claim 1 wherein the embedded controller agent and the embedded firmware agent interact to provide security features to the host system.

13. The apparatus of claim 12 wherein the security features are provided prior to the host operating system being loaded.

14. The apparatus of claim 12 wherein the security features are provided after the host operating system has been loaded.

15. The apparatus of claim 12 wherein the security features are provided concurrently with loading of the host operating system.

16. The apparatus of claim 12 wherein the security features comprise performing verification of the host system and selectively reporting results to a remote device via the embedded controller agent.

17. The apparatus of claim 12 wherein the security features comprise performing virus recovery operations via the embedded controller agent.

18. The apparatus of claim 12 wherein the security features comprise providing authentication services for the host system via the embedded controller agent.

19. The apparatus of claim 12 wherein the security features comprise providing support for mutual authentication of a network communication session.

20. A method comprising:

invoking a management mode in a host system in which a host operating system temporarily relinquishes control of the host system with an embedded controller agent having a network connection that operates independently of the host operating system; and

servicing requests from the embedded controller agent during the management mode with an embedded firmware agent by communicating with the embedded controller agent over a bi-directional agent bus.

21. The method of claim 20 wherein the embedded firmware agent services requests from the embedded controller agent by interacting with a trusted module to provide cryptographic operations.

22. The method of claim 20 wherein invoking the management mode comprises:

asserting a management interrupt with the embedded controller agent; and

entering the management mode in response to the management interrupt.

23. The method of claim 20 wherein the embedded controller agent and the embedded firmware agent interact to provide manageability features to the host system.

24. The method of claim 23 wherein the manageability features are provided prior to the host operating system being loaded.

25. The method of claim 23 wherein the manageability features are provided after the host operating system has been loaded.

26. The method of claim 23 wherein the manageability features are provided concurrently with loading of the host operating system.

27. The method of claim 23 wherein the manageability features comprise host operating system independent update of a flash memory device via the embedded controller agent.

28. The method of claim 23 wherein the manageability features comprise monitoring of host functionality and reporting to a remote device via the embedded controller agent.

29. The method of claim 23 wherein the manageability features comprise providing boot services to the host system via the embedded controller agent.

30. The method of claim 23 wherein the manageability features comprise providing emergency runtime services via the embedded controller agent.

31. The method of claim 20 wherein the embedded controller agent and the embedded firmware agent interact to provide security features to the host system.

32. The method of claim 31 wherein the security features are provided prior to the host operating system being loaded.

33. The method of claim 31 wherein the security features are provided after the host operating system has been loaded.

34. The method of claim 31 wherein the security features are provided concurrently with loading of the host operating system.

35. The method of claim 31 wherein the security features comprise performing verification of the host system and selectively reporting results to a remote device via the embedded controller agent.

36. The method of claim 31 wherein the security features comprise performing virus recovery operations via the embedded controller agent.

37. The method of claim 31 wherein the security features comprise providing authentication services for the host system via the embedded controller agent.

38. The method of claim 31 wherein the security features comprise providing support for mutual authentication of a network communication session.

39. An article comprising a computer-readable medium having stored thereon instructions that, when executed, cause one or more processing elements to:

invoke a management mode in a host system in which a host operating system temporarily relinquishes control of the host system with an embedded controller agent having a network connection that operates independently of the host operating system; and

service requests from the embedded controller agent during the management mode with an embedded firmware agent by communicating with the embedded controller agent over a bi-directional agent bus.

40. The article of claim 39 wherein the embedded firmware agent services requests from the embedded controller agent by interacting with a trusted module to provide cryptographic operations.

41. The article of claim 39 wherein the instructions that cause the one or more processing elements to invoke the management mode comprise instructions that, when executed, cause the one or more processing elements to:

assert a management interrupt with the embedded controller agent; and

enter the management mode in response to the management interrupt.

42. The article of claim 39 wherein the embedded controller agent and the embedded firmware agent interact to provide manageability features to the host system.

43. The article of claim 42 wherein the manageability features are provided prior to the host operating system being loaded.

44. The article of claim 42 wherein the manageability features are provided after the host operating system has been loaded.

45. The article of claim 42 wherein the manageability features are provided concurrently with loading of the host operating system.

46. The article of claim 42 wherein the manageability features comprise host operating system independent update of a flash memory device via the embedded controller agent.

47. The article of claim 42 wherein the manageability features comprise monitoring of host functionality and reporting to a remote device via the embedded controller agent.

48. The article of claim 42 wherein the manageability features comprise providing boot services to the host system via the embedded controller agent.

49. The article of claim 42 wherein the manageability features comprise providing emergency runtime services via the embedded controller agent.

50. The article of claim 39 wherein the embedded controller agent and the embedded firmware agent interact to provide security features to the host system.

51. The article of claim 50 wherein the security features are provided prior to the host operating system being loaded.

52. The article of claim 50 wherein the security features are provided after the host operating system has been loaded.

53. The article of claim 50 wherein the security features are provided concurrently with loading of the host operating system.

54. The article of claim 50 wherein the security features comprise performing verification of the host system and selectively reporting results to a remote device via the embedded controller agent.

55. The article of claim 50 wherein the security features comprise performing virus recovery operations via the embedded controller agent.

56. The article of claim 50 wherein the security features comprise providing authentication services for the host system via the embedded controller agent.

57. The article of claim 50 wherein the security features comprise providing support for mutual authentication of a network communication session.

58. A system comprising:

a bus;

a digital signal processor coupled with the bus;

an embedded firmware agent coupled with the bus having instructions that cause the embedded firmware agent to selectively operate in a management mode during which a host operating system relinquishes control of a host system in which the embedded firmware agent resides;

an embedded controller agent that operates independently of the host operating system and selectively invokes the management mode, the embedded controller agent having a network interface to allow the embedded controller agent to communicate over a network independently of the host operating system; and

a bi-directional agent bus coupled between the embedded firmware agent and the embedded controller agent to transmit messages between the embedded firmware agent and the embedded controller agent.

59. The system of claim 58 further comprising a trusted module coupled with the embedded firmware agent and the embedded controller agent, the trusted module to perform cryptographic operations to support operations by the embedded controller agent.

60. The system of claim 58 wherein the embedded controller agent asserts a management interrupt signal to invoke the management mode.

61. The system of claim 58 wherein the embedded controller agent and the embedded firmware agent interact to provide manageability features to the host system.

62. The system of claim 61 wherein the manageability features are provided prior to the host operating system being loaded.

63. The system of claim 61 wherein the manageability features are provided after the host operating system has been loaded.

64. The system of claim 61 wherein the manageability features are provided concurrently with loading of the host operating system.

65. The system of claim 61 wherein the manageability features comprise host operating system independent update of a flash memory device via the embedded controller agent.

66. The system of claim 61 wherein the manageability features comprise monitoring of host functionality and reporting to a remote device via the embedded controller agent.

67. The system of claim 61 wherein the manageability features comprise providing boot services to the host system via the embedded controller agent.

68. The system of claim 61 wherein the manageability features comprise providing emergency runtime services via the embedded controller agent.

69. The system of claim 58 wherein the embedded controller agent and the embedded firmware agent interact to provide security features to the host system.

70. The system of claim 69 wherein the security features are provided prior to the host operating system being loaded.

71. The system of claim 69 wherein the security features are provided after the host operating system has been loaded.

72. The system of claim 69 wherein the security features are provided concurrently with loading of the host operating system.

73. The system of claim 69 wherein the security features comprise performing verification of the host system and selectively reporting results to a remote device via the embedded controller agent.

74. The system of claim 69 wherein the security features comprise performing virus recovery operations via the embedded controller agent.

75. The system of claim 69 wherein the security features comprise providing authentication services for the host system via the embedded controller agent.

76. The system of claim 69 wherein the security features comprise providing support for mutual authentication of a network communication session.